GEN 503: Sensitive S&T Supplemental Security Plan and Procedures
July 2020

Background and Purpose

Nearly all of the Lab's scientific and technical activities are exempted from any special security controls by the fundamental research exemption established by National Security Decision Directive 189 of September 21, 1985. The exemption was reinforced by then National Security Director Condoleezza Rice, who wrote to Association of American Universities co-chair Harold Brown in a letter dated November 1, 2001, that "[t]he policy on the transfer of scientific, technical, and engineering information set forth in NSDD-189 shall remain in effect, and we will ensure that this policy is followed." However, special circumstances exist in the Low Energy Recirculator Facility, formerly known as the Free Electron Laser, and some of the engineering activities that may require the creation, sharing, and storage of information and technologies determined to be sensitive.

Science and Technology (S&T) is typically considered to be sensitive if the S&T involves activities or items on the Military Critical Technologies List (MCTL) or if the S&T is included in the Department of State's International Trafficking Arms Regulations (ITAR). Sensitive S&T has consequent export control requirements by law, regulation, and the JLab DOE contract. Some Cooperative Research and Development Activities (CRADA) and Work for Others (WFO) activities may be sensitive as they may have Department of Commerce export control requirements. Mishandling of sensitive S&T can be a violation of federal laws and regulations and have associated legal ramifications.

Jefferson Lab has policies in place for the management of sensitive information and technologies as part of the Lab's Security Plan. The policy that specifically addresses the protection of sensitive information can be found in the Security Plan for Protection of Sensitive Information, link at https://cc.jlab.org/sensitiveinfo.

Technical control plans with explicit controls, procedures, and training are required for sensitive S&T to meet Department of State, Department of Commerce, and Department of Defense regulations. The procedures in this plan provide requirements for those who have access to or could handle sensitive S&T in the course of their duties at Jefferson Lab. This is to assure that similar information and technologies are protected according to statute, policy, and our stakeholders' expectations. These policies and procedures are in addition to the standard security procedures that apply to all S&T at Jefferson Lab.

In addition to the procedures in this document, there may be additional requirements that are unique to specific physical locations, networks, etc. If so, these will be provided by your supervisor.

General Procedures.

1. All areas with sensitive S&T requiring export controls must have an area-specific supplemental security plan that addresses the following items:
    - Physical security, e.g. physical access controls, such as restricting access into sensitive areas by requiring the use of electronic keycards or physical/mechanical keys, controlling storage and use of sensitive materials within their areas of use, and limiting electronic device access.

- Information security, e.g. controlling physical access to documents, locking documents in approved rooms and containers, and appropriately destroying documents by crosscut shredding or disposing in an approved disposal collection container.
- Personnel security involves ensuring that only persons who have appropriate training and an authorized right or need-to-know are able to access to controlled S&T. Examples include contract labor, to include end dates of the contract (Persons should not be given access beyond the end date of the subcontract, CRADA, or WFO). Similarly, non-U.S. citizens should not be given access beyond the end date established by their U.S. Citizenship & Immigration Service and Authority to work documents.
- The training must include personal acknowledgement and acceptance of responsibility to meet the requirements.

2. For all areas that generate, use, or store sensitive S&T where the participation of staff, users, or other collaborators who are non-U.S. persons [1] is required, a documented determination must be made by the Export Control Officer, as to whether a Department of Commerce or Department of State export control license is required for the deemed export, i.e. an export to a non-U.S. person who is in the U.S. For these areas, only non-U.S. persons with appropriate licenses will be allowed to participate in the activities and have access to the information and technologies.
3. At least annually for all areas with scientific and technical sensitive information and technologies, the Lab's Export Control Officer must provide a documented self-assessment of the associated security operations.

Roles and Responsibilities

<u>JLab Export Control Officer and Security Officer</u>

- Consistent with responsibilities detailed in JLab's Export Control Procedures Manual, the Export Control Officer is responsible for reviewing all of the Lab's technology transfer documents such as CRADAs, Work for Others, and cooperative agreements. The Export Control staff serves as a resource to JLab employees in identifying Export Controlled equipment, technologies, and information.
- Maintain the Science and Technology Supplemental Security plan, and act as a resource to areas of management and staff regarding sensitive and potentially sensitive S&T.
- Perform periodic reviews of S&T list and policies to assure compliance with security expectations of customers and stakeholders.
- Determines who in the Facilities and Logistics Management Group has access to the sensitive S&T areas and provides their training.
- Export Control Procedures can be found at http://www.jlab.org/intralab/security/. Also, contact Shipping and Receiving (5010) for assistance.

<u>Division Leaders</u>

- Review science and technology in consultation with funding programs, technical experts, and the Export Control Officer to determine what is sensitive. Along with principal investigators,

[1] A U.S. person is a citizen of the United States, a lawful permanent resident alien of the U.S. (a "green card holder"), a refugee, protected political Asylee or someone granted temporary residency under amnesty or Special Agricultural Worker provisions. The general rule is that only U.S. persons are eligible to receive controlled items, information or software without first obtaining an export license from the appropriate agency.

lead scientists, and stake holders disclose in writing potential sensitive S&T information and technologies in all technology transfer planning documents.

- Determine who in the Division is permitted access to sensitive science and technology. Some personnel outside the initiating Division who support sensitive S&T and operations may also be designated as part of this list.
- Assure that all personnel have been properly trained and that policies and procedures regarding sensitive S&T are adhered to.

Chief Information Officer

- Provide systems designs, procedures, reviews, etc. for IT systems containing sensitive S&T.
- Determines who in the Computational Sciences & Technology Division has access to sensitive S&T.

Designated Personnel

- Potential sensitive Scientific and Technical information and technologies must be disclosed in writing in the technology transfer documents by the principal investigator or lead scientist.
- Manage sensitive S&T in accordance with Jefferson Lab security procedures.
- Complete training as required to handle sensitive S&T including acknowledgement of responsibilities.

All Personnel

- All personnel are responsible to identify to their supervisor if they believe they are involved with handling sensitive S&T.

Required Handling of Sensitive S&T

Hard Copy Information

- Mark any sensitive information documents that you create, as provided by your Division and supervisor for your specific program.
- Hard copies of sensitive materials must be locked in filing cabinets when not in use by approved personnel. Sensitive materials, including S&T, are not permitted to be out of cabinets during normal working hours except in areas where prior approval to do so has been given.
    - Sensitive S&T documents that are hand-carried out of the normal work area must be concealed in an unmarked protective folder and properly controlled by a responsible person at all times.
    - Sensitive S&T documents in use must be protected from casual viewing by unauthorized persons through physical control of the work area.
- Sensitive S&T hard copies must be destroyed by shredding in a crosscut shredder or given to the Lab Security Officer for destruction.
- Many documents from DOD only have the FOUO marking. Some of them have DoD Distribution Statements; see: https://discover.dtic.mil/wp-content/uploads/2018/09/distribution_statements_and_reasonsSept2018.pdf for submission guidelines.
- Unclassified information throughout the executive branch that requires safeguarding or dissemination control may be designated as Controlled Unclassified Information (CUI) and

will be marked accordingly. For further information about CUI, see the Lab's Security Plan for Protection of Sensitive Information.

- If the activity involves a Department of Commerce export control license, then the documents should be marked "Business Sensitive –Export Controlled."
- Each CRADA or WFO with Department of Commerce export controlled or proprietary information must include information security in its security plan.

Electronic Information

- All shared sensitive S&T electronic information and electronic systems must be managed and accessed according to the specific plans and procedures provided by your Division and supervisor.
- Any removable media, such as backup CDs, memory sticks, etc. with sensitive S&T must be treated the same as hard copies.
    - If the activity involves a Department of Commerce export control license, then the associated CRADA or WFO will include electronic information in its security plan.

Email

- The Lab's email system can store / process sensitive information. However, the body of the messages or the attachments or both (as appropriate) should be encrypted as provided by your Division and supervisor for your specific program.
- As receipt of email with sensitive S&T cannot be controlled, users are responsible not to read sensitive S&T emails on devices that are not properly configured for sensitive information. Users should set up sensitive subfolders for sensitive S&T, immediately move any incoming sensitive S&T email to one of these folders, and never read sensitive S&T on devices not pre-approved for this use, such as mobile devices or any device not owned and managed by the JLab Computational Sciences & Technology Division.
- Many email clients (Outlook, Mac Mail, Thunderbird, etc.) are configured with default settings that automatically move copies of all email including attachments onto the local system. The Lab's Office 365 (O365) email system does not do this if the web browser interface is used. Any time an insecure system is used to read Lab email, users should close the browser and clear the cache before allowing anyone else to use the computer. Before reading Lab email on an insecure system such as a home computer or personal cell phone, contact the Computer Center for assistance in configuring it so as to not have copies of the email stored on an insecure computer or device.

Release to Other Parties

- Sensitive S&T may not be released outside the Lab unless first approved via the two step process:
    - Concurrence by the appropriate Division Head, and
    - Executing the standard review process by the cognizant program authority.

Personnel

- Export control licenses are sought from either Department of Commerce or Department of State as appropriate to cover non-U.S. persons working on sensitive S&T.
    - Non-U.S. persons may not work on export controlled sensitive S&T without a license.

- Conversations, exchange of information, etc. regarding sensitive S&T can only be with appropriate DOD or DOE personnel including their contractors, or with JLab personnel on the approved list.
    - A given CRADA or WFO activity will typically specify who has access to materials and information used for those specific projects.
- Division Heads can provide clarification for those who have questions about what is appropriate.

Physical Security

- Detailed physical security plans and procedures will be provided by the appropriate Division via the supervisors.

Jefferson Lab Course GEN 503

I acknowledge and understand that sensitive science and technology (S&T) data may be subject to export control restrictions under Jefferson Science Associates', management and operating contract with the U.S. Department of Energy, as well as applicable laws and regulations from the U.S. Department of Commerce or Department of State. I understand the policies, supplemental plan and procedures for management of this sensitive S&T data. Failure to follow these procedures may result in disciplinary action up to and including termination from the Lab. Such violations may also result in criminal prosecution as specified by federal laws and regulations.

Click and enter your information to complete this training and your certification.